REMARKS

The present Amendment amends claims 1, 7 and 15, and leaves claims 2-6 and 16-19 unchanged. Therefore, the present application has pending claims 1-7 and 15-19.

Applicants acknowledge the Examiner's indication in the Office Action that claim 7 would be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims. Amendments were made to claim 7 to place it in independent form including all the limitations of the base claim and any intervening claims. Therefore, claim 7 is now allowable as indicated by the Examiner.

Claims 1-6 and 15-19 stand rejected under 35 USC §103(a) as being unpatentable over Schneier (a portion of a text book entitled "Applied Cryptography") in view of Barton (U.S. Patent No. 5,912,972). This rejection is traversed for the following reasons. Applicants submit that the features of the present invention as now more clearly recited in 1-6 and 15-19 are not taught or suggested by Schneier or Barton whether taken individually or in combination with each other as suggested by the Examiner. Therefore, Applicants respectfully request the Examiner to reconsider and withdraw this rejection.

A simple clarifying amendment was made to each of independent claims 1 and 15 so as to emphasize what is already recited in the claims, namely that the partial image forms a part of the original image from which it has been processed. Applicants submit that this amendment does not change the scope of the claims requiring further consideration and/or search on the part of the Examiner. This

amendment merely clarifies the intent of Applicants, specifically that the partial image is part of the original image and as such is used in a manner so validate the whole of the original image. Such features are clearly not taught or suggested by any of the references of record, particularly Schneier and Barton whether taken individually or in combination with each other as suggested by the Examiner.

Applicants submit that various arguments were presented distinguishing the features of the present invention as recited in the claims from Schneier and Barton in the Remarks of the December 2, 2004 Amendment. The Remarks of the December 2, 2004 Amendment are incorporated herein by reference. In said Remarks, it was shown that Schneier does not teach or suggest the producing of a partial image from an original image and the transmitting of the partial image with a direct and an indirect product of the original whole image using public key cryptography to ensure the authenticity of the partial image in connection with the original whole image as in the present invention. The Examiner agrees with this assessment and specifically states in the Office Action that:

> "Schneier is silent on a first step of processing said original image so as to produce partial image, a fourth step of merging said partial image in said first signed data, applying a one-way function to the merged data, and ciphering an output of said one-way function with a secret key of said data transmission side so as to obtain said second signed data and said ciphered signed data to the data reception".

However, in the Office Action the Examiner attempts to supply the above noted deficiencies of Schneier with teachings in Barton. Specifically, the Examiner points to a teaching in Barton in col. 6, lines 66-67 and alleges that this passage of Barton corresponds to the first step of processing the original image to produce

image as in the present invention as recited in the claims. This passage of Barton is not in anyway related to the processing of an original whole image so as to obtain a partial image which forms a part of the original whole image as in the present invention. This teaching of Schneier is merely directed to the embedding of a bit string such a meta-data to each data block wherein the meta-data could be a block sequence number of information that identifies the creator of the block or the licensing agent.

Specifically, Barton teaches in col. 6, line 55 through col. 7, line 3 that an:

> "embedding process is shown in Fig. 1. A control process invokes the embedding process on an appropriate data block. For each data block, the control process presents the data block and an additional bit string that may contain meta-data that is to be embedded along with the basic authentication information. The meta-data may be block sequence number, and it may also include other meta-data, such as a bit string that identifies the creator or the block or the licensing agent. The embedding process modifies the data block in place to contain the embedded information. The steps of the embedding process are:
>
> 1. calculate a digital signature for the block (10). The bits modified by the embedding process in the digital signature calculation are not included because they will change. This is easily done by assuming that those modified bits were all zeros or all one for the purposes of the computation".

Thus, rather than disclosing that a partial image is obtained by processing the whole image as in the present invention, Barton simply discloses that in the signature calculation 10 bits to be modified by the embedding process are excluded.

This is not in anyway equivalent a partial image of a whole image as in the present invention as recited in the claims.

According to the present invention, a partial image has significance in that it must be guaranteed, at the receiving end, that it is unaltered from the partial image generated at the transmission side, as well as that it is authentically a part of the "whole image". Barton is not clear about the relationship between the alleged (partial) data block and the original whole data block. In fact, there is no description at all in Barton regarding the relationship between each data block and a whole image as in the present invention as recited in the claims. Thus, it is not clear how Barton's data block (partial) is guaranteed to be authentically a part of an original whole image since no such original whole image is discussed. Therefore, there is no teaching in Barton of a "partial image" equivalent to the "partial image" as in the present invention as recited in the claims.

A graphical illustration of the features of the present invention as recited in the claims is provided by the attached Sketch 1. Also, a graphical illustration of the teachings of Barton are supplied by the attached Sketch 2. A simple comparison of the elements of these two sketches clearly shows the difference in functionality of the present invention as recited in the claims relative to the teachings of Barton.

Even if the data block taught by Barton, after excluding a part to be modified, could be considered a "partial image", then the calculation of the digital signature as per Barton is performed on the partial image to produce a signed partial data rather than the whole image as in the present inventions as recited in the claims. This teaching of Barton is in contradiction to the digital signature processing performed on

the whole image, thereby producing the signed whole data as in the present invention as recited in the claims. Thus, Barton does not have a partial image and a first signed data for the process of merging partial and whole images as recited in the claims. Instead, Barton merges a signed partial data with (unsigned) meta-data quite different from the present invention as recited in the claims.

Therefore, the present invention can guarantee a higher level of security than Barton. With the use of the present invention, it can be confirmed that the received partial image DB is unaltered from the transmitted partial image DB, and that the received partial image indeed comes from the whole image from which the signed data SB and the ciphered signed data SAE were generated. In the method of Barton, the authenticity of the meta-data in connection with the data block needs to be guaranteed by some means other than the scheme described using the attached diagram.

In order to understand the advantages of the present invention as claimed, suppose the transmitted set of data is intercepted by someone with the malicious intent of tampering with the data, particularly so that the receiving side would think that the partial data DB comes from another (wrong) whole image. This would be critical in situations where, for example, medical imaging or important birth records are passed between offices as described on page 3 of the present invention. This problem is not addressed in Barton.

With Barton's method, the interceptor needs only to tamper with the ciphered data to fake the origin of the data block. To do this, he only needs to decipher the ciphered data and detach the data block (which he would already know because he

can intercept it along with the ciphered data) to extract the meta-data, and replace it with a fake meta-data and merge it back with the data block, cipher it again, then transmit it with the data block.

The present invention provides much more difficulty for the interceptor. First, to fake the origin of the partial image, the interceptor would need to tamper with all the information derived using the whole image, i.e., signed data SB and ciphered signed data SAE. Thus, in the situation of the present invention in order to generate a fake signed data SB* and a fake ciphered signed data SAE*, the following procedure is necessary:

- decipher the intercepted ciphered signed data SAE using B's secret key (not disclosed, unlike the public key) to obtain signed data 1 SA
- generate a fake signed data 1 SA*
- cipher SA* with B's public key to produce fake ciphered signed data SAE*
- merge SA* with the partial image DB, operate a one-way function on the merged data, and then cipher the merged data with A's secret key to produce fake singed data 2 SB*

In all, the interceptor needs to know two secret keys (one being of the transmitting side and the other being of the receiving side), along with the one-way hash function. The generation of a fake signed data SA* will also present more difficulty for the interceptor compared with the meta-data of Barton. The examples of meta-data of Barton are listed in col. 2, lines 63-65. These can be faked quite easily, compared to a signed data.

Thus, as is quite clear from the above, both Schneier and Barton fail to teach or suggest a first step of processing the original image so as to produce a partial

image which forms a part of the original image, a second step of applying a digital signature to the original image so as to produce first signed data, and a third step of ciphering the first signed data with a public key of the data reception side so as to produce a ciphered signed data as recited in the claims.

Further, both Schneier and Barton fail to teach or suggest a fourth step of merging the partial image and the first signed data, applying a one-way function to the merged data and ciphering an output of the one-way function with a secret key of the data transmission side so as to obtain second signed data and a fifth step of transmitting the partial image, the second signed data and the ciphered signed data to the reception side as recited in the claims.

Still further, both Schneier and Barton fail to teach or suggest a seventh step of deciphering the obtained ciphered signed data with a secret key of the data reception side so as to obtain third signed data and an eighth step of merging the obtained partial image and the third signed data and applying a one-way function to the merged data as recited in the claims.

Even further still, both Schneier and Barton fail to teach or suggest a ninth step of deciphering the received second signed data with a private key of the data transmission side and a tenth step of comparing results of the eighth and ninth steps so as to verify data validity as recited in the claims.

Therefore, since both Schneier and Barton are deficient of the same features of the present invention as recited in the claims, the combination of said references do not teach or suggest the features of the present invention as now more clearly recited in the claims. Accordingly, reconsideration and withdrawal of the 35 USC

§103(a) rejection of claims 1-6 and 15-19 as being unpatentable over Schneier in view of Barton is respectfully requested.

The remaining references of record have been studied. Applicants submit that they do not supply any of the deficiencies noted above with respect to the references utilized in the rejection of claims 1-6 and 15-19.

In view of the foregoing amendments and remarks, applicants submit that claims 1-7 and 15-19 are in condition for allowance. Accordingly, early allowance of claims 1-7 and 15-19 is respectfully requested.

To the extent necessary, the applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger, Malur & Brundidge, P.C., Deposit Account No. 50-1417 (500.39507X00).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/jdc
(703) 684-1120